UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/666,632	09/18/2003	Ernie F. Brickell	42P17256	8964

8791 7590 08/04/2009
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
KANAAN, SIMON P	
ART UNIT	**PAPER NUMBER**
2432	
MAIL DATE	**DELIVERY MODE**
08/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/666,632	**Applicant(s)** BRICKELL, ERNIE F.
	Examiner SIMON KANAAN	**Art Unit** 2432

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13 and 24-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-10,12,13 and 24-27,29,30* is/are rejected.

7)☒ Claim(s) *4,11 and 28* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *9/18/2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 10666632 filed on 04/21/2009 is presented for examination by the examiner.

Election/Restrictions

2. Claims 10-13 and 27-30 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected species, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 4/21/2009.

Drawings

3. The applicant's drawings submitted are acceptable for examination purposes.

Information Disclosure Statement

4. The information disclosure statements (IDS) submitted on 12/6/2006 and 3/17/2005 have been acknowledged. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 4 and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Regarding claims 4 and 11, the phrase "multiplying a quantity by a selected bit of the exponent plus one, the quantity comprising a message minus one" renders the claim indefinite because it is unclear whether the "plus one" is computed before or after the multiplication.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1-3, 5-9, and 24-26, are rejected under 35 U.S.C. 102(b) as being anticipated by Kocher et al. (US PATENT # 6,298,442 B1).

As per claims 1 and 24, Kocher discloses a method and article for obscuring cryptographic computations comprising: performing modular exponentiation in a cryptographic computation such that memory accesses are independent of the numerical value of the exponent. – Kocher, Column 12, lines 1-3.

As per claims 2 and 25, Kocher discloses the method and article of claims 1 and 24 respectively, wherein performing modular exponentiation comprises replacing a conditional multiplication operation with an unconditional multiplication operation. - Kocher, Column 3, lines 42-49, exponentiation using conditional multiplication is replaced with exponentiation which is unconditional.

As per claim 3, Kocher discloses the method of claim 2, wherein the unconditional multiplication operation uses an obscuring factor. - Kocher, Column 3, lines 50-54, modular exponentiation is performed with fixed memory access patterns which are an obscuring factor

As per claim 5, Kocher discloses the method of claim 1, wherein the exponent comprises at least one of a signature exponent and a decryption exponent in a RSA cryptographic system, and the cryptographic computation is at least one of signature and decryption. - Kocher, Column 12, lines 10-11, RSA is used as the asymmetric cryptographic protocol.

As per claim 6, Kocher discloses the method of claim 5, wherein the cryptographic computation comprises c^d mod n, wherein c comprises a ciphertext message, d comprises the decryption exponent, and n comprises a modulus that is a product of two prime numbers. - Kocher, Column 4, lines 10-25, cryptographic computation comprises x^y mod n where x is equivalent to c, y is equivalent to d and n is a composite number which is the product of two prime numbers.

As per claim 7, Kocher discloses the method of claim 1, wherein the modular exponentiation is performed as part of a Diffie-Hellman key exchange process. - Kocher, Column 12, lines 15-16, Diffie-Hellman is used as the asymmetric cryptographic protocal.

As per claim 8, Kocher discloses the method of claim 1, wherein the modular exponentiation is performed as part of a Digital Signature Algorithm (DSA) process. - Kocher, Column 12, lines 13-14, DSA is used as the asymmetric cryptographic protocal.

As per claims 9 and 26, Kocher discloses the method and article of claims 1 and 24 respectively, further comprising applying a window method as part of performing the modular exponentiation and retrieving pre-computed powers from one to 2^v of a message from a memory, where v is the size of a window into the exponent's bits. - Kocher, Column 4, lines 45-66, performing modular exponentiation comprises retrieving pre-computed values from a table i.e. window, where the table size is dependent on the exponent.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claim 4, 10-13, and 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Curiger et al. (US Patent # 6,064,740).

As per claims 10 and 27, Kocher discloses a method and article for obscuring cryptographic computations by performing modular exponentiation of an exponent in a cryptographic computation such that memory accesses are independent of the exponent bit pattern comprising:

but fails to explicitly disclose setting an intermediate value to a message; and for each bit i in the exponent, setting the intermediate value to the intermediate value multiplied by the intermediate value mod a modulus, wherein the modulus comprises a product of two prime numbers, determining a current obscuring factor using the i'th bit of the exponent, and setting the intermediate value to the intermediate value multiplied by the current obscuring factor mod the modulus.

However, Curiger discloses setting an intermediate value to a message; and for each bit i in the exponent, setting the intermediate value to the intermediate value multiplied by the intermediate value mod a modulus, wherein the modulus comprises a product of two prime numbers, determining a current obscuring factor using the i'th bit of the exponent, and setting the intermediate value to the intermediate value multiplied by the current obscuring factor mod the modulus. –Curiger, column 12, lines 5-15, an intermediate value is set equal to itself multiplied by itself mod a modulus and then is modded by an obscuring factor.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the obscuring factor as taught by Kocher with obscuring factor as taught by Curiger since Curiger's obscuring method minimizes the processing time. – Curiger, column 11, lines 59-63.

As per claims 12 and 29, Kocher in view of Curiger discloses the method and article of claims 10 and 27 respectively, wherein the exponent comprises at least one of a signature exponent and a decryption exponent in a RSA cryptographic system, and the cryptographic computation is at least one of signature and decryption. - Kocher, Column 12, lines 10-11, RSA is used as the asymmetric cryptographic protocol.

As per claims 13 and 30, Kocher in view of Curiger discloses the method and article of claims 10 and 27 respectively, further comprising applying a window method as part of performing the modular exponentiation and retrieving pre-computed powers from one to 2^v of the message from a memory, where v is the size of a window into the exponent's bits. - Kocher, Column 4, lines 45-66, performing modular exponentiation comprises retrieving pre-computed values from a table i.e. window, where the table size is dependent on the exponent.

Allowable Subject Matter

Claims 4, 11 and 28 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571) 270-3906. The examiner can normally be reached on Monday to Friday 8:30 AM to 5:00 PM.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Gilberto Barron, can be reached at the following telephone number: (571) 272-3799.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/SIMON KANAAN/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432